XpoLog Center Suite
Log Management & Analysis platform

Summary:

1. **End to End data management** – collects and indexes data in any format from any machine / device in the environment.
2. **Logs Monitoring** - Automatic monitoring and alerting on rules.
3. **XpoLog Search** – powerful search on all logs including aggregations, statistics and trends analysis.
4. **Analytics (Problems Analysis console)** - Automated problems analysis and monitoring engine.
5. **Dashboards / Reporting** - custom live Dashboards – visualization of logs data

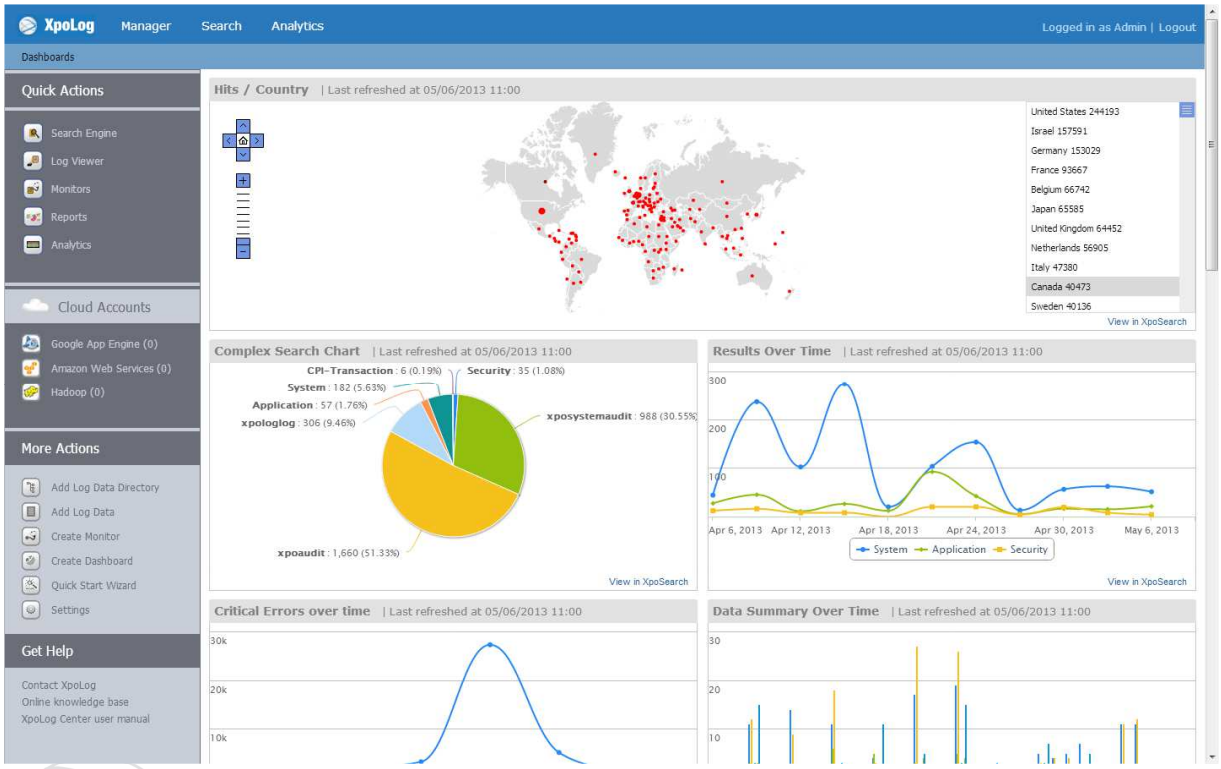
Visit our online knowledge base – http://wiki.xpolog.com
For more information, product demo or anything else that may assist with please don't hesitate to contact us at support@xpolog.com

Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

General

XpoLog Center software suite includes the following modules:

1. **XpoLog Manager** - administration wizards and consoles for log management - mapping log sources, data collection and archiving, authentication and authorization settings and more.
2. **XpoLog Search** - Google like search for logs, single point of search using queries and complex queries to quickly view all matching log events, create aggregation and ad-hoc visualization.
3. **Analytics** - Log problems mapped over time - Automated analysis on all log sources for fast problem isolation and efficient troubleshooting..



Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com

XPLG

General

XpoLog is a data analysis and management platform for Applications IT data. Business applications running on modern data centers rely on highly dynamic heterogeneous applications infrastructure like cloud and virtualization. Organization's critical technology operations generates huge volumes of IT machine generated data, this Big Data contains critical information on problems, faults, quality issues, security threats, operational and application intelligence, users behavior and more.

XpoLog data analysis and management platform helps to collect, manage, analyze and search this cryptic unstructured Big Data.
XpoLog collects, indexes and correlates data in a searchable repository from which it can generate graphs, reports, alerts, dashboards and visualizations. The platform delivers application and operational intelligence to application owners, operations, IT administrators, cloud services consumers and other stakeholders across the IT life cycle.
XpoLog recent Augmented Search technology brings intelligence amplification concepts that harness advanced data analytics technology with end user intellect, helping to uncover hidden values in IT Big Data and increase systems quality and availability.

The software installs in less than 5 minutes on any JAVA supported OS, and the system can be accessed by users using any common browser.

Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

XPLG

End to End Data Management

It is simple to map multiple log sources to XpoLog to get relevant data from the environment into XpoLog's repository. Within minutes the data become available, searchable and can be deeply analyzed in a single console.

Data can be collected from UNIX machines, Windows machines, Network and Security devices, Application servers, Databases and more.
Using XpoLog collection policies it is possible to collect data at any given frequency from second upwards, as well as keep the available in the XpoLog repository for as long as needed.

View the System Architecture **here**

Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

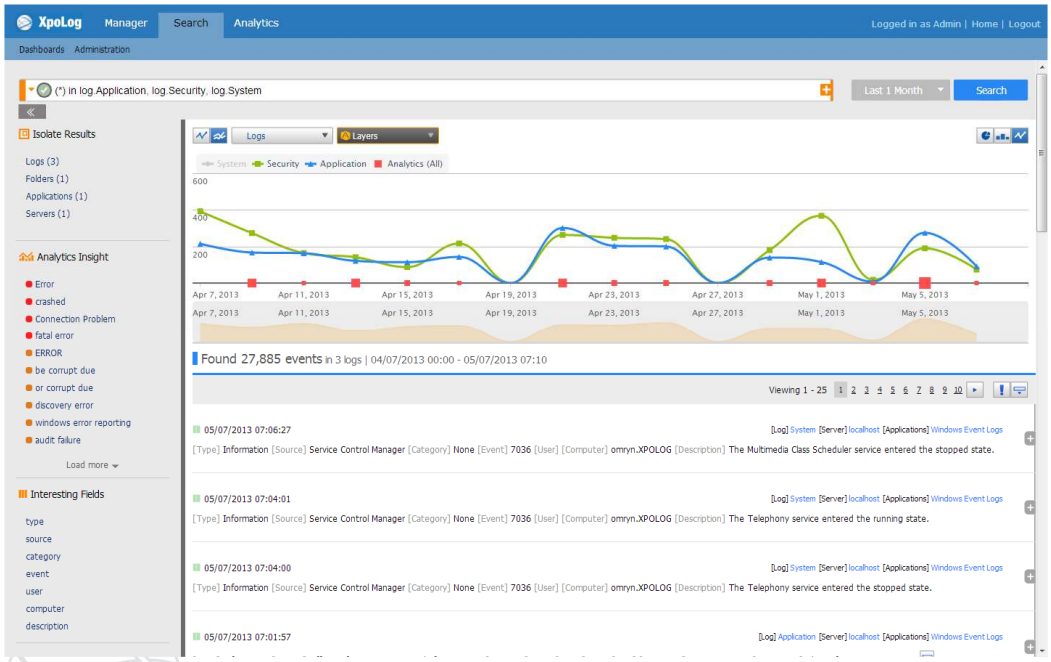
XPLG

XpoLog Search

XpoLog Search is a powerful, distributed search engine that enables users to search all logs from all sources on any time frame, and get matching events presented in a single console within seconds.
The search syntax offers a wide verity of operators (AND, OR, NOT, CONTAIN, = != <>, wild cards, regular expressions and more). The matching events are presented over time and users can quickly zoom in and isolate matching events from any source in any time frame.

XpoLog Augmented search presents knowledge layers of automatic detected problems in the user's search context.

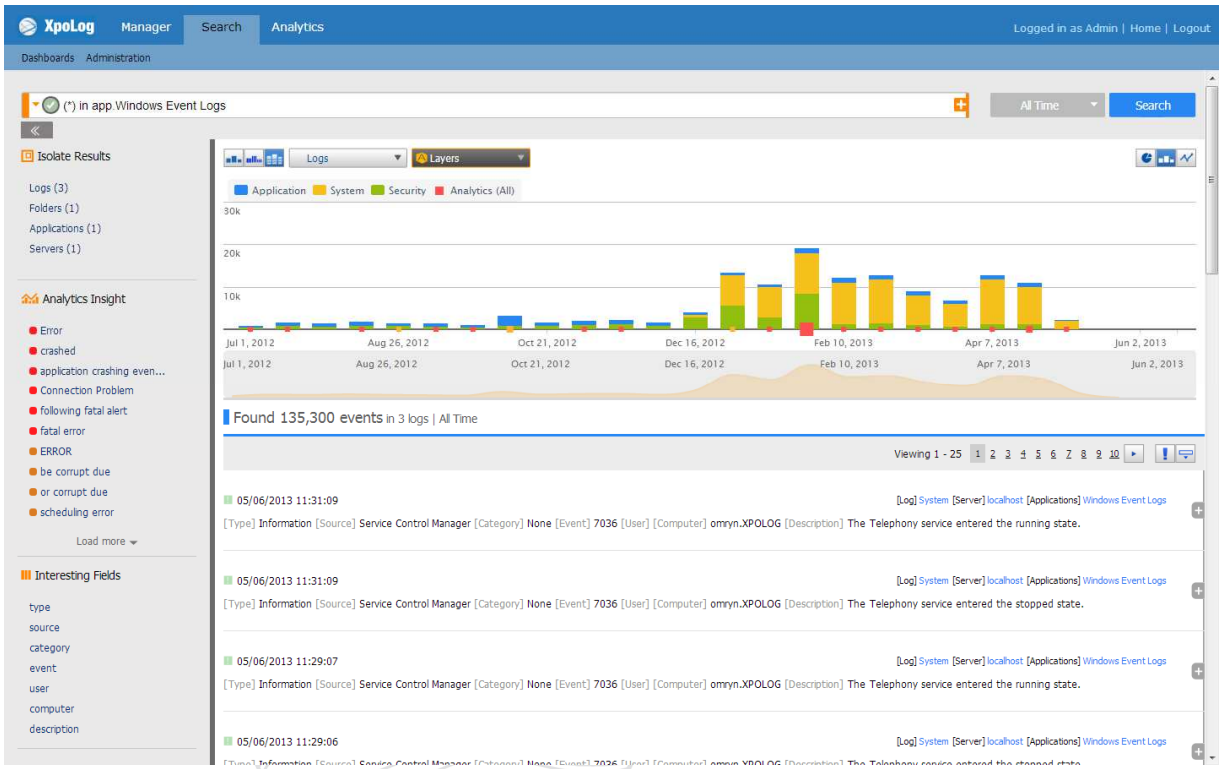
XpoLog Search complex queries provide options to aggregate logs data and generate advanced statistics, trends and business intelligence and transactions analysis (correlations) on the logs data.



Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

Simple Searches
All matching events are presented in the view (latest on top) and an overtime, per log, sources distribution.

Here's an example of running a general search on all Windows logs to get all matching events from all sources available in the console

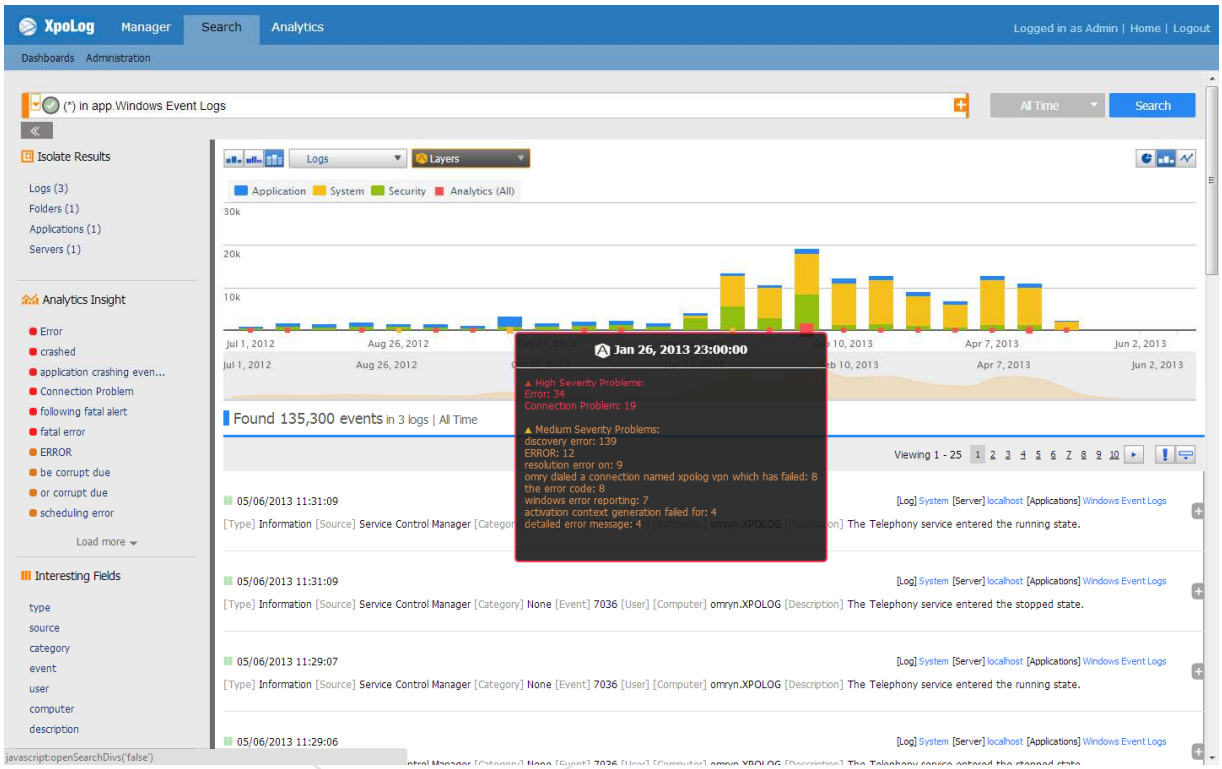


Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

Search Augmentation

XpoLog Search presents problems which were automatically detected by the system under any search context – by a click of the button these hidden problems can be presented in the console.

Here's an example of running a general search on all Windows logs and on top on the result XpoLog automatically suggests problems that were detected tagged to severities



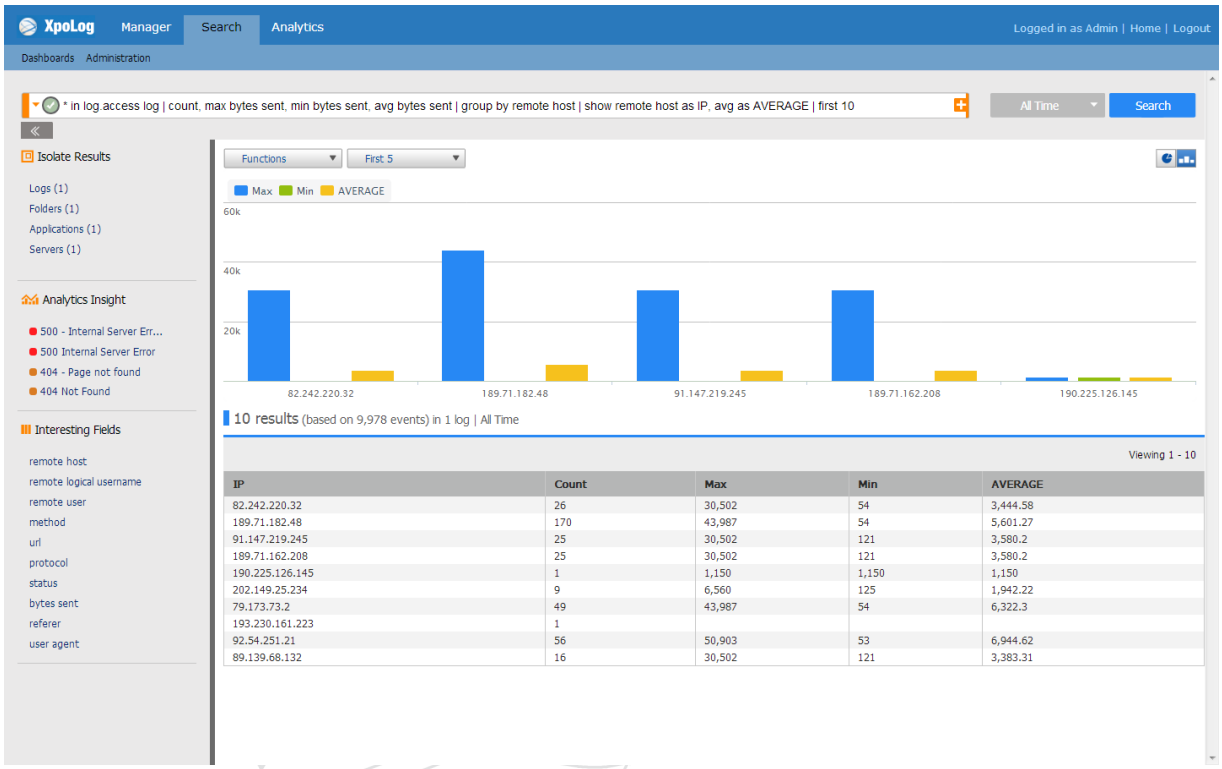
Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

XPLG

Complex Searches

XpoLog Search contains advanced computation and statistics functions that can be activated on any search result. For example count events, calculated averages, see specific distribution by a specific time period and many more.

Here's an example of counting hits of top 10 IP addresses on a site with some statistics on their activity



IP	Count	Max	Min	AVERAGE
82.242.220.32	26	30,502	54	3,444.58
189.71.182.48	170	43,987	54	5,601.27
91.147.219.245	25	30,502	121	3,580.2
189.71.162.208	25	30,502	121	3,580.2
190.225.126.145	1	1,150	1,150	1,150
202.149.25.234	9	6,560	125	1,942.22
79.173.73.2	49	43,987	54	6,322.3
193.230.161.223	1			
92.54.251.21	56	50,903	53	6,944.62
89.139.68.132	16	30,502	121	3,383.31

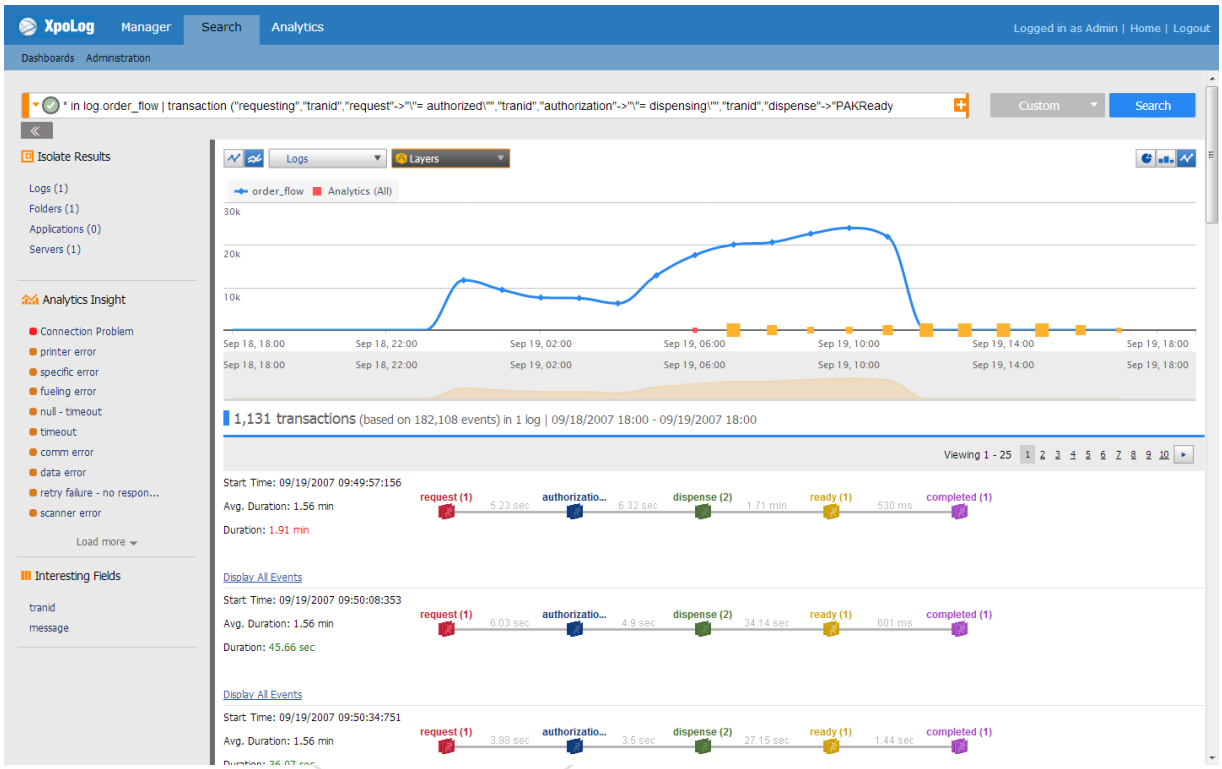
Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

XPLG

Complex Searches – events correlations (Transactions)

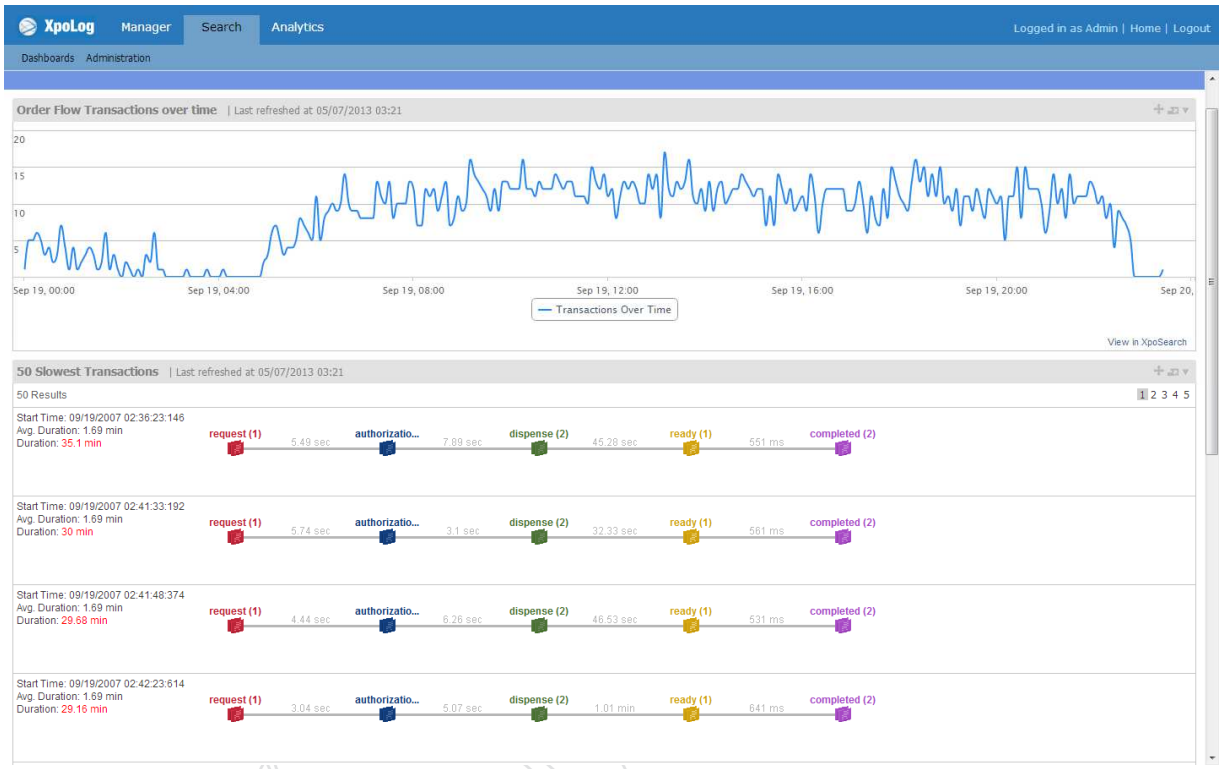
As part of XpoLog Search's complex computation and statistics functions it can map events correlations from multiple sources. The transactions can be analyzed in a very efficiently to measure transactions over time, identify slow transactions, generate statistics and alerts and more.

Here's an example of events correlation



Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com

Here’s an example of events correlation statistics



Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

Analytics (Problems Analysis Console)

The Analytics is a proactive mechanism that scans all logs data and identifies, without any pre-knowledge, critical problems in logs and servers. The Analytics presents a unified analysis report of all logs, based on several criteria's:

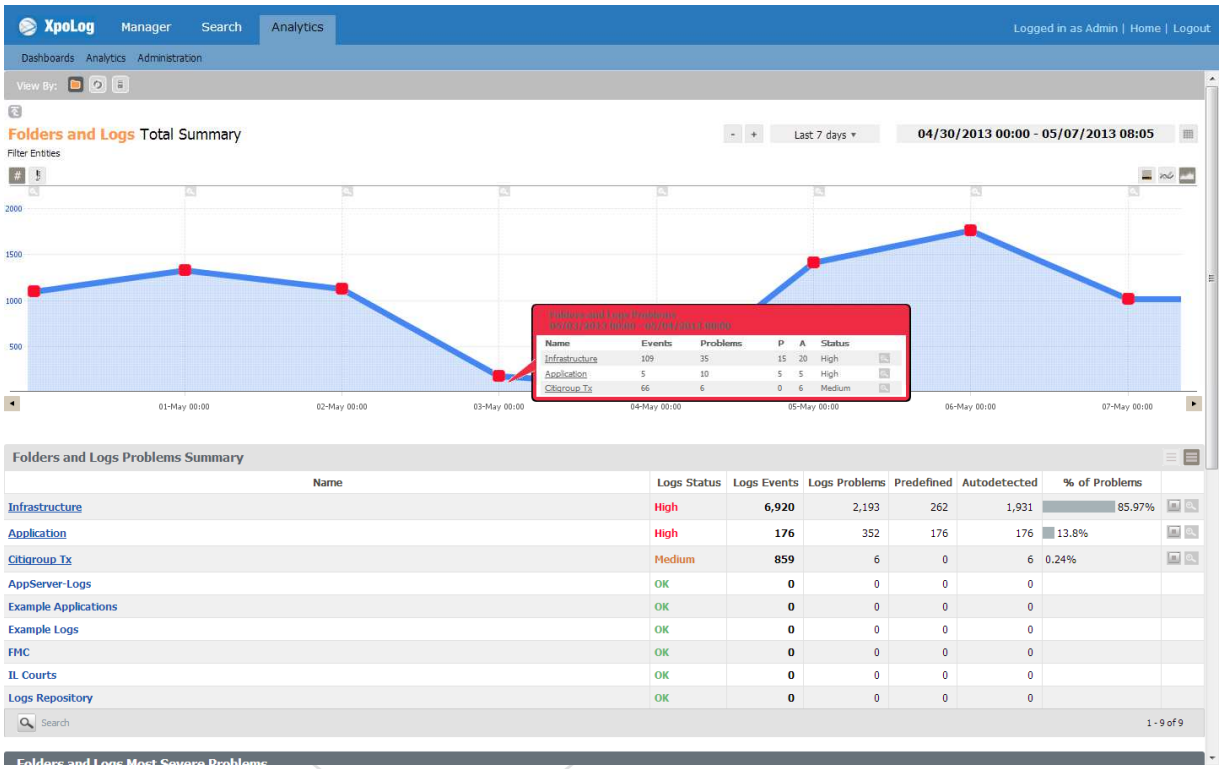
1. Problems Analysis - General applications behavior presented over time. The Analytics maps problems over time on a log level or application level over time.
   Log problems are listed with drill down links to the log events.
   A user can select a preferred view type (per log, per application or per server) and quickly navigate between different sources over any desired time frame
2. Risk Level Analysis - Each problem indication that the Analytics presents is tagged to a severity. A severity on an automatic detected problems is assigned by XpoLog (and can be easily modified by users) or by the users as predefined problems that added to the system.

The Analytics console is integrated to XpoLog Search in augmented search knowledge layers. Problems which the Analytics engine detects automatically appear on top of the search results in the XpoLog Search console.

Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

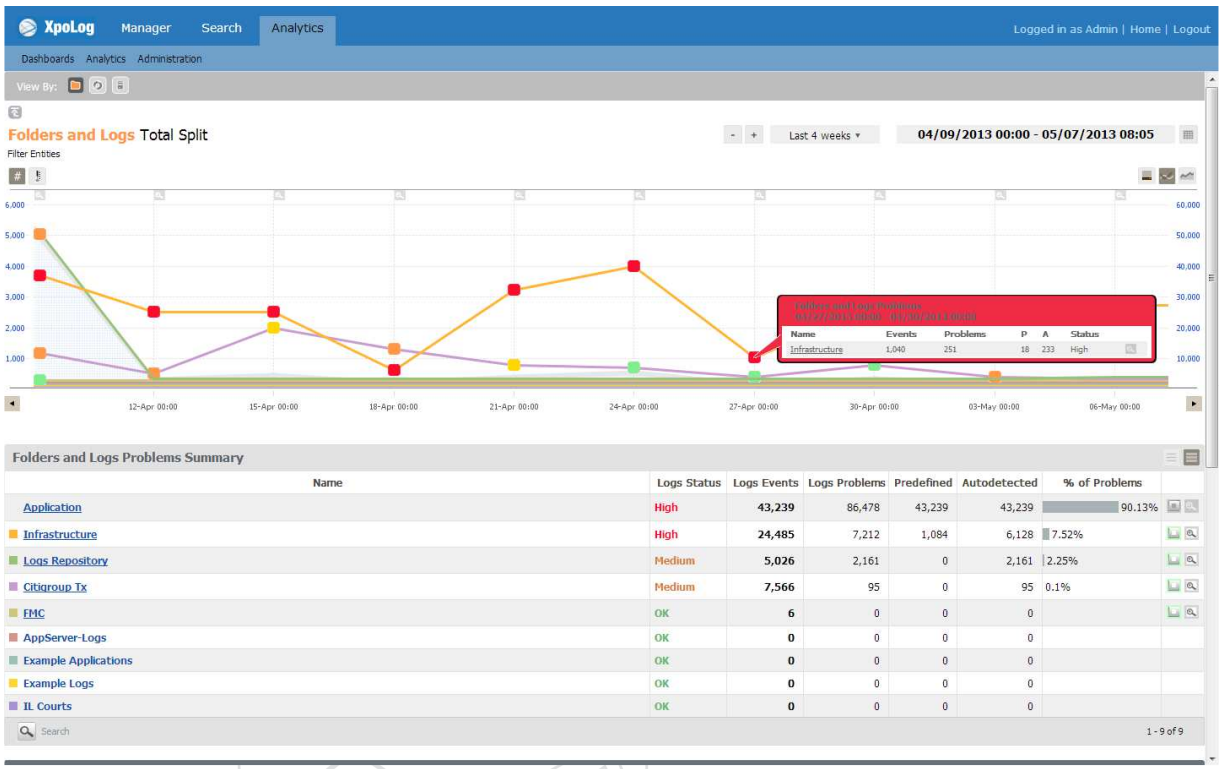
Problems over Time
For any time frame, the Analytics presents the log volume and detected problems tagged to severities. Problems severity levels are: None (green), Low (yellow), Medium (orange), and High (red).

Summary (aggregated view):
Default view – problems mapped over time and details on each source below with top problems. Users can quickly change presented time frame, drill down for specific source, or replace views (see below).



Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

Split View (problems analysis per source view):
At any given view, users can select a split view to see the analysis individually per each log source and the problems that were detected per source.
The Problems Analysis is integrated to XpoLog Search to enable fast drill down from a captured problem indication into the event view.

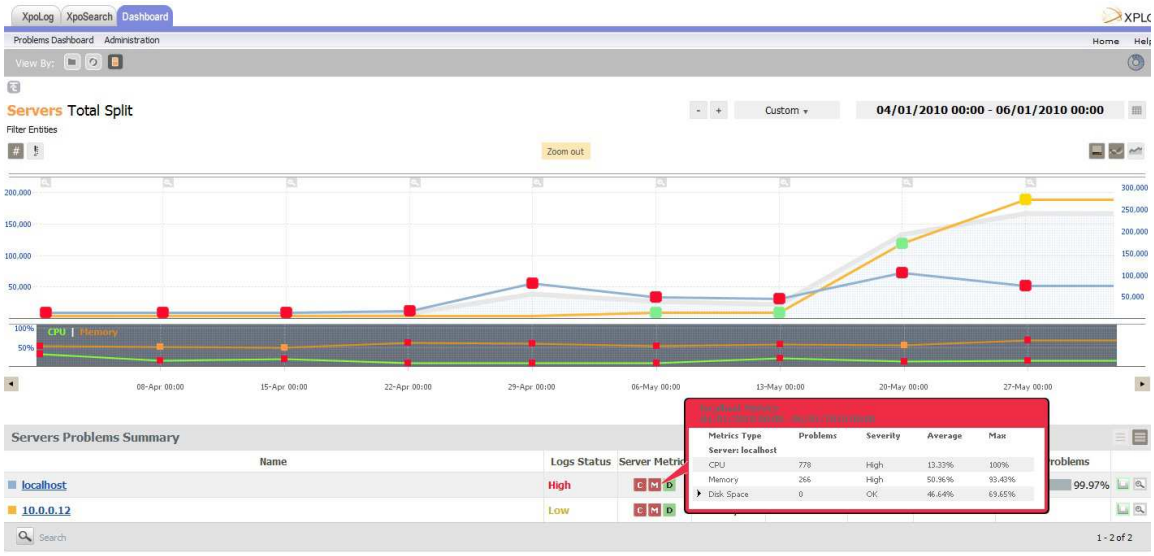


Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

Metrics Measurements and Monitoring

The Analytics can also measure CPU level, memory level and available disk space from all remote servers that XpoLog is connected to. The measurement interval and problems definitions are completely configurable and may be changed.

Metrics problems, like any other logs problems, may trigger alerts to indicate problems.



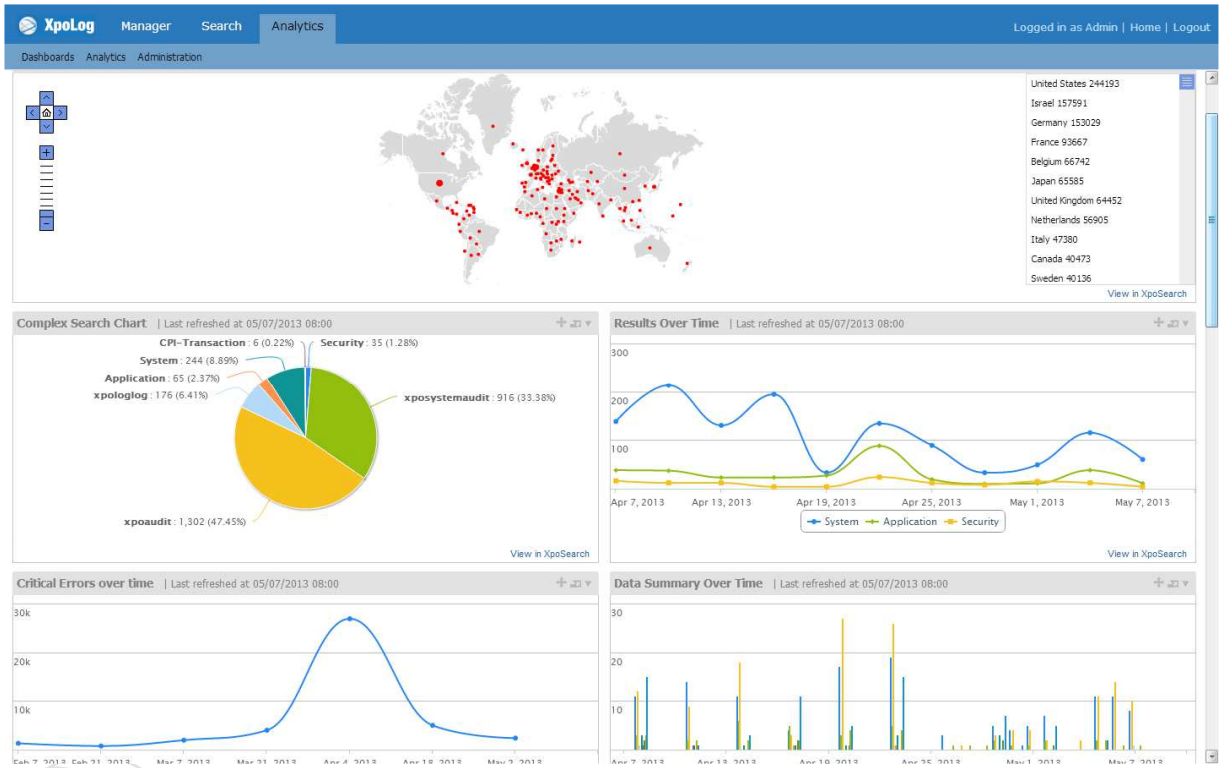
Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com

Dashboards

XpoLog contains a Dashboards engine. Users can save multiple customized Dashboards to visualize anything from the logs – search results, reports results, complex search result, Analytics analysis, correlations results and more.

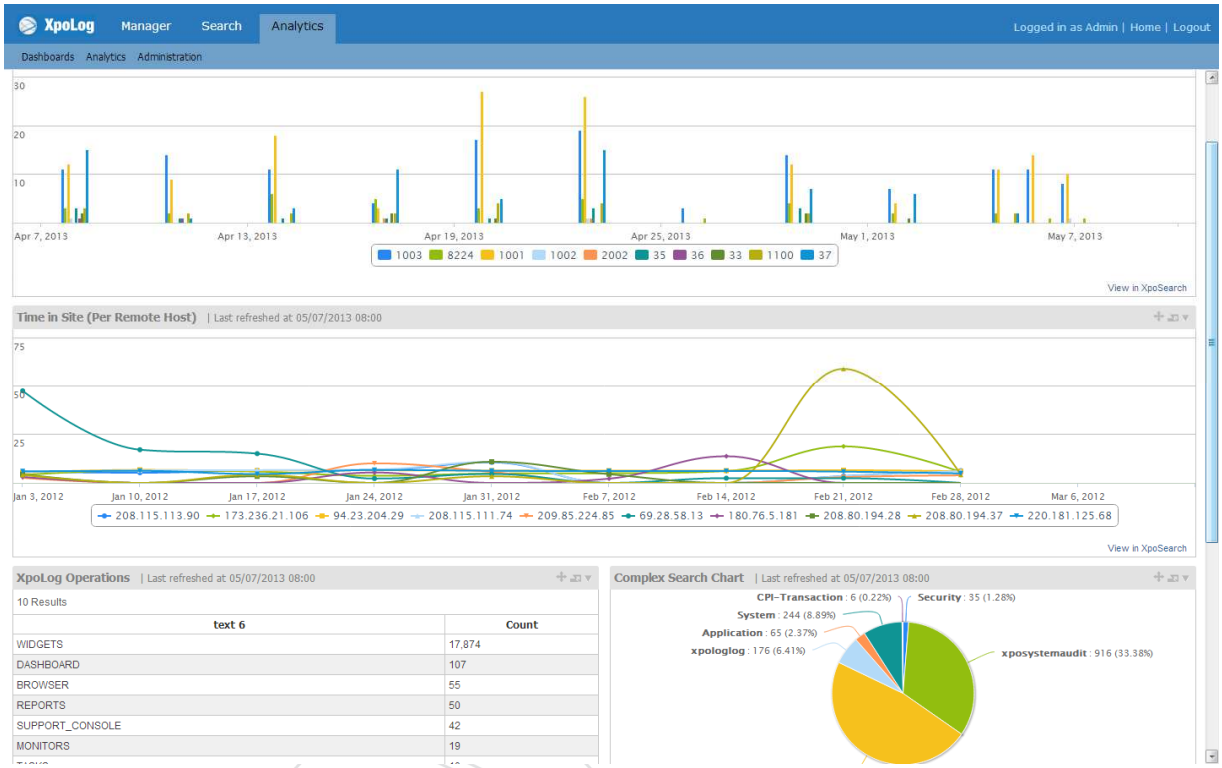
Data can be visualized in many forms - pie charts, line charts, bar charts, stack charts, events list and more. Dashboards can be exported to PDF by demand or automatically as reports to the relevant groups.

Example I – web analysis, GEO-IP map, and more:



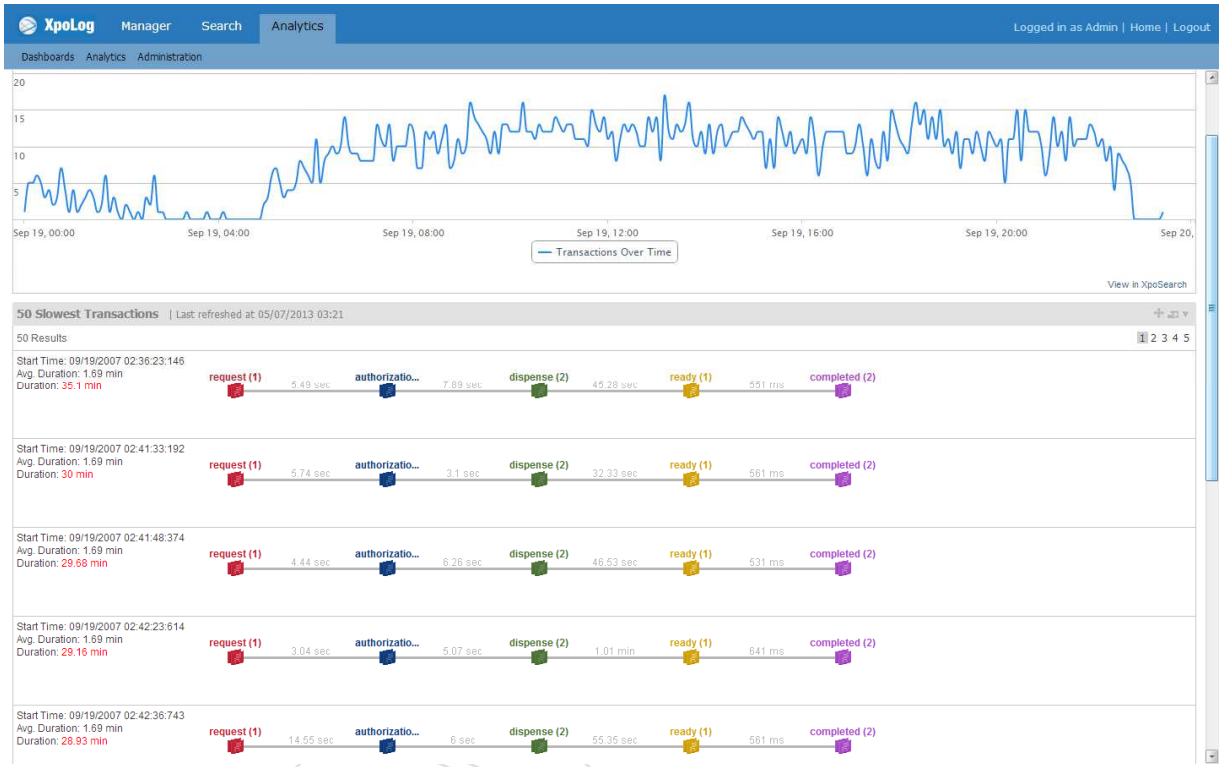
Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com

Example II – application analysis:



Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM

Example III – Transaction analysis:



Tel: +972 3 634 3884
Fax: +972 3 542 3226
Kfar Truman 1, 73150
P.O.B 174, Israel
Email: info@xplg.com
WWW.XPLG.COM